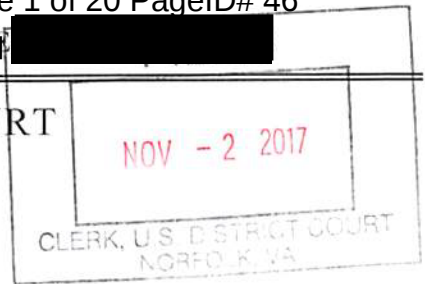


UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia



In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Information associated with the Dropbox, Inc. accounts)
associated with a) user name john wo and e-mail address)
johninnorfolk@gmail.com, and b) user name: mike fall and e-mail)
address mikefall25@gmail.com, that is stored at premises owned,)
maintained, controlled, or operated by Dropbox,)
Inc., a company whose custodian of records is located at)
185 Berry Street, Suite 400, San Francisco, California 94107)
(Pursuant to 18 U.S.C. § 2703 and Fed. R. Crim. P. 41.))

Case No. 2:17sw 179

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location): **See Attachment A-1.**

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
See Attachment A-2.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	Offense Description
18 U.S.C. § 2252(a)(1)	Transportation of Child Pornography
18 U.S.C. § 2252(a)(2)	Receipt and/or Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts: **See Affidavit.**

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

Elizabeth M. Yusi
Assistant United States Attorney

Applicant's signature
Kristin B. Joseph, Special Agent, Homeland Security Investigations
Printed name and title

Sworn to before me and signed in my presence.

Date: 11-2-17
City and state: Norfolk, VA

Lawrence R. Leonard
United States Magistrate Judge

ATTACHMENT A-1

Accounts to Be Searched

This warrant applies to all information associated with the Dropbox Inc. accounts associated with the Dropbox Inc. accounts associated with a) user name: john wo and e-mail address johninnorfolk@gmail.com, and b) user name: mike fall and e-mail address mikefall25@gmail.com (the SUBJECT ACCOUNTS), from 2013 to the present, that is or was stored at the premises owned, maintained, controlled, or operated by DROPBOX INC. whose custodian of records is located at 185 Berry Street, Suite 400, San Francisco, California 94107. The information should include any information preserved pursuant to the preservation request made on November 1, 2017, pursuant to 18 U.S.C. § 2703(f), by Assistant United States Attorney Elizabeth M. Yusi and with Dropbox Inc. reference number CR-6000-4114.

VB LRL

ATTACHMENT A-2

Particular Things to be Seized

I. Information to be disclosed by Dropbox Inc.

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Dropbox Inc. (Dropbox), including any messages, records, files, logs, or information that have been deleted but are still available to Dropbox or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox is required to disclose the following information to the government for the SUBJECT ACCOUNTS listed in Attachment A-1 from 2013 to the present:

a. The contents of all folders associated with the account, including stored or preserved copies of files sent to and from the account, the source and destination addresses associated with file, and the date and time at which each file was sent;

b. All transactional information of all activity of the Dropbox accounts described above, including log files, messaging logs, records of session times and durations, dates and times of connecting, and methods of connecting; and emails "invites" sent or received via Dropbox, and any contact lists.

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Dropbox and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, files, and electronic messages, that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1), (a)(2), and (a)(4), including, for the SUBJECT ACCOUNTS, information pertaining to the following matters:

a. Any person knowingly transporting distributing, receiving or possessing child pornography;

- b. Credit card and other financial information including but not limited to bills and payment records;
- c. Evidence of who used, owned, or controlled the accounts or identifiers listed on Attachment A-1 ;
- d. Evidence of the times the accounts or identifiers listed on Attachment A-1 was used;
- e. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A-1 and other associated accounts

III. Method of delivery

Notwithstanding 18 U.S.C. § 2252, Dropbox shall disclose responsive data, if any, by delivering encrypted files on any digital media device to Special Agent Kristin Joseph located at the address Homeland Security Investigations, 200 Granby Street, Suite 600, Norfolk, Virginia 23510.

In Re Search Of:

- 1) Information associated with the DROPBOX INC. accounts associated with a) user name: john wo and e-mail address johninnorfolk@gmail.com, and b) user name: mike fall and e-mail address mikefall25@gmail.com, that is stored at premises owned, maintained, controlled, or operated by DROPBOX INC. whose custodian of records is located at 185 Berry Street, Suite 400, San Francisco, California 94107.
- 2) Information associated with the GOOGLE INC. accounts associated with e-mail address johninnorfolk@gmail.com and e-mail address mikefall25@gmail.com, that is stored at premises owned, maintained, controlled, or operated by GOOGLE INC. whose custodian of records is located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

2:17sw 179
2:17sw

AFFIDAVIT

INTRODUCTION AND AGENT BACKGROUND

I, Kristin B. Joseph, being first duly sworn state:

1. I am a Special Agent of the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), currently assigned to the Office of the Assistant Special Agent in Charge (ASAC), Norfolk, Virginia. I have been so employed since August 2005. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography¹ including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in all forms of media including computer media. I am also a certified forensic computer examiner for HSI.

SUBJECT ACCOUNTS

¹ "Child Pornography means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8).

(Signature) *LR*

2. This affidavit is made in support of an application for search warrants for the following items (the SUBJECT ACCOUNTS):

- a) Information associated with the DROPBOX INC. accounts associated with a) user name: john wo and e-mail address johninnorfolk@gmail.com, and b) user name: mike fall and e-mail address mikefall25@gmail.com, that is stored at premises owned, maintained, controlled, or operated by DROPBOX INC. whose custodian of records is located at 185 Berry Street, Suite 400, San Francisco, California 94107. The information to be searched and seized is described in the following paragraphs and in Attachments A1 and A2.
- b) Information associated with the GOOGLE INC. accounts associated with e-mail address johninnorfolk@gmail.com and e-mail address mikefall25@gmail.com, that is stored at premises owned, maintained, controlled, or operated by GOOGLE INC. whose custodian of records is located at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachments B1 and B2.

3. This affidavit is made, in part, in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require DROPBOX INC. and GOOGLE INC. to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

4. The information contained in this Affidavit is based on my personal knowledge, the review of documents, and observations made by me during the course of this investigation, as well as, information conveyed to me by other individuals, including information obtained from other law enforcement agencies. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for search warrants, this Affidavit does not set forth each and every fact learned by me or observed by me during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1), 2252(a)(2), and 2252(a)(4) are within the SUBJECT ACCOUNTS.

LEGAL AUTHORITY

A. Pertinent Criminal Statutes

5. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

6. 18 U.S.C. § 2252(a)(2) provides that any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct, shall be punished.

7. 18 U.S.C. § 2252(a)(4) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer.

B. Other Legal Authority

8. The legal authority for this search warrant application regarding the GOOGLE INC. and DROPBOX INC. accounts is derived from 18 U.S.C. §§ 2701-2711, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides in relevant part as follows:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

9. 18 U.S.C. § 2703(b) provides in relevant part as follows:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant.

 LRL

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –

(A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

10. The government may also obtain records relating to e-mail communications, such as subscriber identifying information, by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A).

11. 18 U.S.C. §§ 2703(b)(1)(A) and 2703(c)(1)(A) allow for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

12. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated below. *See* 18 U.S.C. § 3237(a); *see also* 18 U.S.C. §§ 3231 and 3232. *See United States v. Bagnell*, 679 F.2d 826, 830 (11th Cir. 1982) (venue is proper in child pornography and obscenity prosecution in district where images were either distributed or received).

DEFINITIONS

13. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

14. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. For purposes of this affidavit, I use the term “child pornography” interchangeably with “images of minors engaging in sexually explicit activity.”

15. “Cloud-based storage service” or “cloud storage” as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to

their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

16. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

17. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

18. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

19. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

20. “Internet Protocol Address” (IP Address), as used herein, refers to refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

21. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range

of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

22. “Minor” and “sexually explicit conduct” are defined in 18 U.S.C. §§ 2256(1) and (2). A “minor” is defined as “any person under the age of eighteen years.” The term “sexually explicit conduct” means actual or simulated:

- a. Sexual intercourse, including genital genital, oral genital, anal genital, or oral anal, whether between persons of the same or opposite sex;
- b. Bestiality;
- c. Masturbation;
- d. Sadistic or masochistic abuse; or
- e. Lascivious exhibition of the genitals or pubic area of any person.

23. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

25. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

26. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

TECHNICAL BACKGROUND

A. DROPBOX INC.

27. “Dropbox” refers to an online storage medium on the internet accessed from a computer or electronic storage device. As an example, online storage mediums such as Dropbox make it possible for the user to have access to saved files without the requirement of storing said files on their own computer or other electronic storage device. Dropbox is an “offsite” storage medium for data that can be viewed at any time from any device capable of accessing the internet. Users can store their files on Dropbox and avoid having the files appear on their computer. Anyone searching an individual’s computer that utilizes Dropbox would not be able to view these files if the user opted only to store them at an offsite such as Dropbox. These are often viewed as advantageous for collectors of child pornography in that they can enjoy an added level of anonymity and security.

28. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an e-mail

address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

29. When the subscriber transfers a file to a Dropbox account, it is initiated at the user's computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

30. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

31. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

B. GOOGLE INC.

32. E-mail is an electronic form of communication which usually contains written correspondence and graphic images. It is similar to conventional paper mail in that it is addressed from one individual to another and is usually considered private. An e-mail usually contains a message "header" which generally displays the sender's e-mail address, the recipient's e-mail address, and the date and time of the e-mail transmission.

33. If a sender chooses to do so, he or she can type a subject line into the header. E-mail message "headers" usually contain information, such as identification of the sender's ISP, which enables law enforcement officers to trace the message back to the original sender. In order to do so, information must be obtained from the sender's ISP through a Grand Jury or administrative subpoena.

34. GOOGLE INC. is, among other things, a U.S.-based Internet Service Provider or "Web Host." GOOGLE INC. provides a full range of services including but not limited to: web based

e-mail accounts, search engines, directories, travel resources, commercial services, and advertising. GOOGLE INC. provides individuals with free web based e-mail accounts and Instant Messaging services.

35. In my training and experience, I have learned that Google provides a variety of on-line services, including e-mail access, to the general public. Subscribers obtain an account by registering with GOOGLE INC. During the registration process, GOOGLE INC. asks subscribers to provide basic personal information. Therefore, the computers of the companies are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for GOOGLE INC.'s subscribers) and information concerning subscribers and their use of GOOGLE INC.'s services, such as account access information, e-mail transaction information, and account application information.

36. In general, an e-mail that is sent to GOOGLE INC.'s subscribers is stored in the subscriber's "mail box" on GOOGLE INC.'s servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on GOOGLE INC.'s servers indefinitely.

37. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to GOOGLE INC.'s servers, and then transmitted to its end destination. GOOGLE INC. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from GOOGLE INC.'s servers, the e-mail can remain on the system indefinitely.

38. GOOGLE INC.'s subscribers can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by the companies.

39. Subscribers to GOOGLE INC. might not store on their home computers copies of the e-mails stored in their account. This is particularly true when they access their account through the web, or if they do not wish to maintain particular e-mails or files in their residence. Google gives users 15 GB of storage, which is equivalent to store over 970,000 eight-page Word documents. As a result, most users do not delete a large portion of their e-mails.

40. Google Drive, formerly Google Docs, is a file storage and synchronization service created by GOOGLE INC. This is where the 15GB of storage mentioned in the preceding paragraph is housed. It allows users to store files in the cloud, share files, and edit documents, spreadsheets, and presentations with collaborators.

41. In general, e-mail providers like the companies ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

42. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the

account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via GOOGLE INC.'s websites), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

43. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

44. In my training and experience, evidence of who was using an e-mail account and Instant Messenger accounts may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

45. "Photo-Sharing service" or "photo-sharing website" is a service that allows the publishing or transfer of a user's digital photo online, thus enabling the user to share them with others, publicly and/or privately. The function is provided through both websites and applications that facilitate the upload and display of images.

46. Picasa is an image organizer and image viewer for organizing and editing digital photos, plus an integrated photo-sharing website, owned by Google.

47. YouTube is a video-sharing website owned, operated, and controlled by Google, on which users can upload share, and view videos. A registered user of YouTube creates a username and provides certain identifying information to YouTube, including the user's e-mail address. Registered users of YouTube create usernames. Unregistered users can watch the videos, but only registered users are permitted to upload videos, including amateur content such as short original videos.

48. Registered and unregistered users of YouTube can e-mail hyperlinks of the posted videos to others. All YouTube users can also post "user comments" about the videos. The uploading of videos containing child pornography is prohibited by YouTube's terms of service agreement with users. YouTube allows users to file reports if a user believes that a video is inappropriate.

49. In addition, I know that Google provides web hosting, either for free or through paid services. Google provides design services for the customer's website, hosting, and e-mail capability through these services.

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

50. Based upon my training and experience and information officially supplied to me by other law enforcement officers, I know the following:

- a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 64 gigabytes of data or more, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.
- c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through FTPs to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
- d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte (1,000 GB's) external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital

 LRL

camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person.

- e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as GOOGLE INC. and DROPBOX INC., among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.
- g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

PROBABLE CAUSE

51. On August 4, 2016, an adult relative of defendant Robert Michael Fall went to the Virginia Beach Police Department (VBPD) to report that she found images of minors engaging in sexually explicit conduct (SEC) on an HP laptop computer, S/N CNF03787FC, belonging to Fall. The relative had been staying at Fall’s residence in Virginia Beach and had access to Fall’s computers. She brought one of Fall’s computers to the VBPD, the HP laptop computer, S/N CNF03787FC, to show the police an example of the images and turn over the computer to VBPD. The relative stated that Fall had additional computers and computer media at his residence.

52. Detectives with VBPD immediately went to Fall’s work to interview him. After being given his *Miranda* rights, Fall refused to speak with the detectives. During the same time period, VBPD police officers were sent to Fall’s residence in order to freeze the scene pending a search warrant.

53. That same day, VBPD obtained a search warrant for Fall’s residence and executed it on the same day. During the search warrant, a neighbor reported that he saw someone place a

(Handwritten signature/initials) LRL

computer on the rooftop of Fall's house prior to the execution of the search warrant while VBPD police officers were in front of the residence. VBPD retrieved the computer from the roof, which was an additional HP laptop computer, S/N 5CG2152NK. VBPD also seized other computers and numerous DVDs and CDs from Fall's bedroom. A forensic analysis of the HP laptop computers, a Dell computer, and numerous DVDs and CDs revealed over 3,000 images of minors engaging in SEC, including images that depicted sadistic and masochistic conduct of minors.

54. Fall's child pornography activity, based on the dates on the computers and other media, goes back to 2002. This means that Fall was collecting child pornography for well over ten years.

55. Fall was arrested by VBPD that same day and was held with no bail.

56. The forensic analysis shows that in at least March and April 2016, Fall was using DROPBOX INC. to upload and/or download images of child pornography. While the majority of the images and/or videos were not able to be viewed because they had been deleted from the computer media, the names of the files being moved to and/or from DROPBOX INC. account(s) are indicative of images and/or videos depicting child pornography. For example, some of the file names being saved to or downloaded from DROPBOX INC. included:

- a. "Pthc 2010yo with dad showing her pussy from the rear"
- b. "Pthc Hussyfan Kingpass Vicky Lordofthering Moscow Liluplanet Nablot St Petersburg R@Ygold Babyshivid 0Ann Holliday - Tryng Fuck 3 10Yo Vw-03.avi"
- c. " new pthc laura anal closeup"

57. The video listed was "Pthc 10yo with dad showing her pussy from the rear.3gp," "(Pthc) (Hussyfan) (Kingpass) (Vicky) (Lordofthering) (Moscow) (Liluplanet) (Nablot) (St Petersburg) (R@Ygold) (Babyshivid) Ann Holliday - Tryng Fuck 3 10Yo (Vw-03).avi." The latter video also appeared on the desktop of one of Fall's computers as well as on one of the CDs/DVDs found in his bedroom. The video is approximately 20 minutes in length and depicts a girl that appears to be between 4 and 6 years old having sexual intercourse with an adult male.

58. On February 8, 2017, a grand jury in the United States District Court for the Eastern District of Virginia, Norfolk, returned a five-count indictment against Fall, charging him with receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(2) and (a)(4). The state charges against Fall were nolle prossed and he was transferred to federal custody. Fall has been detained pending trial in this matter and has not had access to the Internet.

59. On October 12, 2017, a grand jury in the same court returned a nine-count superseding indictment against Fall charging him with transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(1), (a)(2) and (a)(4). The same grand jury returned a second superseding indictment on November 1, 2017, charging Fall with the same

 LRL

counts. Trial is set before the Honorable Senior Judge Henry Coke Morgan, Jr. on December 5, 2017.

60. On or about October 23, 2017, a Court Order under 18 U.S.C. § 2703(d) was served on DROPBOX INC. for the account information associated with the listed Dropbox hyperlinks that appeared to transmit images of child pornography found on Fall's computers. On or about October 26, 2017, DROPBOX INC. responded to the Court Order indicating that the below listed account was responsible for hosting the links discovered during the forensic analysis.

Name: john wo
E-mail: johninnorfolk@gmail.com
User ID: 480839992
Joined: Sat, 17 Oct 2015 22:11:03 GMT

61. The account was listed as still "active" and the links that were sent to DROPBOX INC. were still active. It also appears that the "john wo" user paid a fee to DROPBOX INC. using a credit card with an associated zip code that was the same zip code as Fall's business.

62. The forensic analysis also revealed that an e-mail account of mikefall25@gmail.com was frequently utilized on the computers seized from Fall.

63. On or about February 21, 2017, HSI issued an administrative summons to DROPBOX INC. for an account associated with the e-mail account of mikefall25@gmail.com. DROPBOX INC. responded to the summons on or about March 13, 2017 and indicated that the below listed account is associated with the e-mail address of mikefall25@gmail.com

Name: mike fall
E-mail: mikefall25@gmail.com
User ID: 480840268
Joined: Sat, 17 Oct 2015 22:12:35 GMT

64. On or about September 1, 2017, HSI issued another administrative summons to DROPBOX INC. for an account associated with the e-mail account of mikefall25@gmail.com. DROPBOX INC. responded to the summons on or about September 7, 2017 and indicated the same information as listed above.

65. Notably, both DROPBOX INC. accounts were opened within minutes of each other.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO TRANSPORT RECEIVE, DISTRIBUTE, OR POSSESS CHILD PORNOGRAPHY

66. Through my training and experience, and through discussions with other law enforcement officers who specialize in the investigation of child pornography, and of subjects who use the Internet to gain access to child pornography, I have learned that individuals who use such technology are often child pornography collectors who download images and videos of child pornography. Moreover, I have learned that many subjects have saved numerous images to their

hard drive, thumb drive, disks or CDs, and have kept that material for long periods of time. Based upon my knowledge, experience and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

- a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, in other visual media or from literature describing such activity.
- b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, drawings, or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Collectors of child pornography typically possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location, such as in cloud storage. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica,² and videotapes for many years.
- d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

² According to former FBI Special Agent Kenneth V. Lanning, the author of a chapter in the book, Child Pornography and Sex Rings, (Lexington Books 1984), a book which deals with the subject of child pornography and pedophiles who collect and produce child pornography, "child erotica" are materials or items which are sexually arousing to pedophiles but which are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions. He defines it in the above book as: any material, relating to children, that is sexually arousing to a given individual...[s]ome of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids. Id. at 83.

LRL


- e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

67. Based on the information herein, I believe that Robert Michael Fall possesses the characteristics common to individuals who collect child pornography. This is based on the length of time he has been collecting child pornography (over 10 years), the amount of child pornography, the number of computer media that contained child pornography, and the fact that he was utilizing cloud services to access child pornography.

CONCLUSION

68. As explained herein, information stored in connection with the SUBJECT ACCOUNTS may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an account user’s profile information, IP log, stored electronic communications, and other data retained by DROPBOX INC. and GOOGLE INC., can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the SUBJECT ACCOUNTS at a relevant time. Further, account activity can show how and when the account was accessed or used. For example, as described herein, DROPBOX INC. and GOOGLE INC. logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Last, account activity may provide relevant insight into the account owner’s state of mind as it relates to the offense under investigation. For example, information on the SUBJECT ACCOUNTS may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

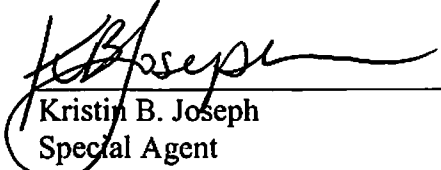
69. Therefore, computers of DROPBOX INC. and GOOGLE INC. are likely to contain all the material described above, including stored electronic information concerning subscribers and

their use of the accounts, such as account access information, transaction information, and other account information.

70. Based on the aforementioned factual information, your affiant respectfully submits that probable cause exists to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(1), (a)(2) and (a)(4) will be found within a) information associated with the DROPBOX, INC. accounts associated with i) user name: john wo and e-mail address johninnorfolk@gmail.com, and ii) user name: mike fall and e-mail address mikefall25@gmail.com, that is stored at premises owned, maintained, controlled, or operated by DROPBOX INC. whose custodian of records is located at 185 Berry Street, Suite 400, San Francisco, California 94107, more particularly described in Attachment A1; and b) information associated with the GOOGLE INC. accounts associated with e-mail address johninnorfolk@gmail.com and e-mail address mikefall25@gmail.com, that is stored at premises owned, maintained, controlled, or operated by GOOGLE INC. whose custodian of records is located at 1600 Amphitheatre Parkway, Mountain View, California 94043, more particularly described in Attachment B1.

71. Accordingly, I request that warrants be issued authorizing your affiant, with assistance from additional HSI agents and other law enforcement personnel, to search the SUBJECT ACCOUNTS, for the items specified in Attachments A2 and B2.

FURTHER AFFIANT SAYETH NOT.



Kristin B. Joseph
Special Agent
Homeland Security Investigations
Norfolk, Virginia

Subscribed and sworn before me on November 2, 2017, in the city of Norfolk, Virginia.



United States Magistrate Judge